UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,783	12/10/2004	Satoshi Kitani	275870US6PCT	8620

22850 7590 04/01/2008

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER
SU, SARAH

ART UNIT	PAPER NUMBER
4158	

NOTIFICATION DATE	DELIVERY MODE
04/01/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/517,783	KITANI ET AL.	
	Examiner	Art Unit	
	Sarah Su	4158	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 December 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☒ Claim(s) *1-4,6-7,10-11,15 and 19-21* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 December 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/10/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Preliminary Amendment received on 10 December 2004, has been entered into record. In this amendment, claim 9 has been amended.

2. Claims 1-22 are presented for examination.

Priority

3. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

4. The information disclosure statement filed 10 December 2004 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because an English equivalent of a portion of the document such as the abstract was not provided. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

Specification

5. Applicant is reminded of the proper content of an abstract of the disclosure. The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The abstract of the disclosure is objected to because it contains more than 150 words. Correction is required. See MPEP § 608.01(b).

6. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

7. The paragraphs of the specification, other than in the claims or abstract, may be numbered at the time the application is filed, and should be individually and consecutively numbered using Arabic numerals, so as to unambiguously identify each paragraph. The number should consist of at least four numerals enclosed in square brackets, including leading zeros (e.g., [0001]). The numbers and enclosing brackets should appear to the right of the left margin as the first item in each paragraph, before the first word of the paragraph, and should be highlighted in bold. A gap, equivalent to approximately four spaces, should follow the number. Nontext elements (e.g., tables, mathematical or chemical formulae, chemical structures, and sequence data) are considered part of the numbered paragraph around or above the elements, and should

not be independently numbered. If a nontext element extends to the left margin, it should not be numbered as a separate and independent paragraph.

A list is also treated as part of the paragraph around or above the list, and should not be independently numbered. Paragraph or section headers (titles), whether abutting the left margin or centered on the page, are not considered paragraphs and should not be numbered. 37 CFR 1.52(b)(6).

8. The disclosure is objected to because of the following informalities:

a. page 27, line 18 “apparatus, but the apparatus” should read –apparatuses, but the apparatuses–;

b. page 72, line 8 “IEEEE1394” should read –IEEE1394–;

c. page 74, line 1 “all but identical” should read –all identical–;

d. page 99, line 13 “521” should read –631–;

e. page 107, line 10 “step 652” should read –step S652–;

f. page 114, line 4 “apparatus even though the apparatus” should read –apparatuses even though the apparatuses–.

g. It appears that the disclosure contains brackets ("[" and "]") around section titles that are nonfunctional (e.g. page 31, line 22). The Examiner requests that these be removed.

Appropriate correction is required.

Claim Objections

9. It is noted that the present application does not contain line numbers in the claims. The preferred format is to number each line of every claim, with each claim beginning with line 1. For ease of reference by both the Examiner and Applicant all future correspondence should include the recommended line numbering. For the purposes of examination, the Examiner has used the preferred format for the remainder of this Office action.

10. Claims 1-4, 6-7, 10-11, 15, 19, 20-21 are objected to because of the following informalities:

a. Claims 1-4 and 6 do not contain proper transitional phrases. See MPEP § 2111.03.

In claim 1:

a. in line 7, “a process” is unclear if it relates to “a process” (claim 1, line 1).

In claim 2:

a. in line 7, “a first block key Kb1” is unclear if it relates to “a first block key Kb1” (claim 1, line 4);

b. in line 9, “a second seed” is unclear if it relates to “a second seed” (claim 1, line 7);

c. in line 9, “a process to decrypt an encrypted second seed” is unclear if it relates to “a process to decrypt an encrypted second seed" (claim 1, line 7);

d. in line 11, “a second block key Kb2” is unclear if it relates to “a second block key Kb2” (claim 1, line 9);

e. in line 13, “encrypted data” is unclear if it relates to “encrypted data” (claim 1, line 2).

In claim 3:

a. in line 6, “a first recording key K1” is unclear if it relates to “first recording key K1” (claim 2, line 8);

b. in line 8, “a second recording key K2” is unclear if it relates to “second recording key K2” (claim 2, line 12).

In claim 4:

a. in line 6, “a first recording key K1” is unclear if it relates to “first recording key K1" (claim 2, line 8);

b. in line 8, “a second recording key K2” is unclear if it relates to “second recording key K2” (claim 2, line 12).

In claim 6:

a. in line 7, “a first block key Kb1” is unclear if it relates to “a first block key Kb1” (claim 5, line 8);

b. in line 9, “a second seed’ is unclear if it relates to “a second seed” (claim 5, line 11);

c. in line 9, “a process to decrypt an encrypted second seed” is unclear if it relates to “a process to decrypt an encrypted second seed” (claim 5, line 11);

d. in line 11, “output-use encrypted information” is unclear if it relates to “output-use encrypted information” (claim 5, line 14).

In claim 7:

a. in line 8, “encrypted information” is unclear if it relates to “encrypted data” (claim 7, line 2);

b. in lines 10 and 12, “encrypted data” is unclear if it relates to “encrypted data” (claim 7, line 2).

In claim 10:

a. in line 2, “encryption-processing units” is unclear if it relates to “encryption-processing units” (claim 9, lines 3-4).

In claim 11:

a. in line 3, “encrypted data” is unclear if it relates to “encrypted data” (claim 9, line 1).

In claim 15:

a. in line 7, “a first block key Kb1” is unclear if it relates to “a first block key Kb1” (claim 14, line 4);

b. in line 9, “a second seed” is unclear if it relates to “a second seed” (claim 14, line 7);

c. in line 9, “a process to decrypt an encrypted second seed” is unclear if it relates to “a process to decrypt an encrypted second seed” (claim 14, line 7);

d. in line 11, “a second block key Kb2” is unclear if it relates to “a second block key Kb2” (claim 14, line 10).

In claim 19:

a. in line 7, “a first block key Kb1” is unclear if it relates to “a first block key Kb1” (claim 18, line 7);

b. in line 9, “a second seed” is unclear if it relates to “a second seed” (claim 18, line 10);

c. in line 9, “a process to decrypt an encrypted second seed” is unclear if it relates to “a process to decrypt an encrypted second seed” (claim 18, line 10);

d. in line 11, “output-use encrypted information” is unclear if it relates to “output-use encrypted information” (claim 18, line 12).

In claim 20:

a. in line 7, “encrypted information” is unclear if it relates to “encrypted data” (claim 20, line 2);

b. in lines 9 and 11, “encrypted data” is unclear if it relates to “encrypted data” (claim 20, line 2).

In claim 21:

a. in line 10, “encrypted data” is unclear if it relates to “encrypted data” (claim 21, line 1).

Appropriate correction is required.

Drawings

11. The drawings in the Preliminary Amendment were received on 10 December 2004. These drawings are Figures 2 and 19.

12. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because:

a. reference characters "221", "521" and “671” have been used to designate DISC ID (Figures 3, 17, 22);

b. reference characters "224" and "524" have both been used to designate TITLE KEY 2 (Figures 3, 17);

c. reference characters "223", "523" and “672” have been used to designate TITLE KEY 1 (Figures 3, 17, 22);

d. reference characters “S112” and “S109” have both been used to designate SELECTOR (Figure 3).

13. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 228 and 528.

14. It is noted that the errors in the drawings are too numerous for the Examiner to particularly specify. The Applicant is reminded of 37 CFR 1.84(p):

(4) The same part of an invention appearing in more than one view of the drawing must always be designated by the same reference character, and the same reference character must never be used to designate different parts.

(5) Reference characters not mentioned in the description shall not appear in the drawings. Reference characters mentioned in the description must appear in the drawings.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version

of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

15. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 9 and 22 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

As to claim 9, the claim is drawn to an arrangement of data per se. Compilations or mere arrangements of data are considered nonfunctional descriptive material because they do not provide any functional interrelationships. Arrangements of data embodied on a computer readable medium or other structure would not be directed to a statutory category of invention since no requisite functionality would be present to satisfy the practical application requirement (see MPEP 2106.01).

As to claim 22, the claim is drawn to a computer program per se. Computer programs claimed as computer listings per se are abstract instructions. Computer programs are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural

and functional interrelationships between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized. As such, these claims are not directed to one of the statutory categories of invention (See MPEP 2106.01), but are directed to nonstatutory functional descriptive material.

Please note that computer programs embodied on a computer readable medium or other structure, which would permit the functionality of the program to be realized, would be directed to a product and be within a statutory category of invention, so long as the computer readable medium is not disclosed as non-statutory subject matter per se (electromagnetic signals or carrier waves).

Claim Rejections - 35 USC § 112

16. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

17. Claims 1-8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 1-8 are directed towards an apparatus and the method steps of using the apparatus, which is ambiguous and thus indefinite. See MPEP § 2173.05(p).

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

20. It is noted that claims 1, 5, 7-9, 14, 18, 20-22 recite intended use (e.g. in claim 1, lines 1-2: "apparatus *used for carrying out a process to decrypt encrypted data stored on an information-recording medium*"). These phrases have been given little patentable weight.

21. Claims 1-4, 9-17, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asano et al. (EP 1185020 A1 and $Asano_1$ hereinafter) in view of Oishi et al. (EP 1039462 A2 and Oishi hereinafter).

22. As to claims 1, 14 and 22, $Asano_1$ discloses a system and method for information recording and reproducing, the system and method having:

generating a first block key Kb1 on the basis of a first seed serving as key generation information set for each of encryption-processing units composing the encrypted data stored on the information-recording medium [claims 1, 14, 22] (0031, lines 2-5);

decrypting the encrypted data stored on the information-recording medium based on the generated second block key Kb2 [claim 1] (0038, lines 2-4; 0052, lines 9-10);

decrypting the encrypted data stored on the information-recording medium by carrying out a decryption process based on the generated second block key Kb2 [claims 14, 22] (0038, lines 2-4; 0052, lines 9-10);

$Asano_1$ does not expressly disclose:

acquiring a second seed by carrying out a process to decrypt an encrypted second seed stored on said information-recording medium on the basis of the generated first block key Kb1 [claims 1, 14, 22];

generating a second block key Kb2 by carrying out an encryption process based on the acquired second seed [claim 1];

generating a second block key Kb2 based on the acquired second seed [claims 14, 22].

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by $Asano_1$, as evidenced by Oishi. Oishi discloses a system and method for encrypted data transfer, the system and method having:

acquiring a second seed (i.e. content key) **by carrying out a process to decrypt an encrypted second seed stored on said information-recording medium on the basis of the generated first block key Kb1** [claims 1, 14, 22] (0009, lines 8-11) in order to allow for the content key to be changed without requiring re-encryption of the data;

generating a second block key Kb2 (i.e. storage encrypted content key) **by carrying out an encryption process based on the acquired second seed** (i.e. content key) [claims 1, 14, 22] (0009, lines 11-15) in order to allow for the content key to be changed without requiring re-encryption of the data.

Given the teaching of Oishi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the system and method of $Asano_1$ with the system and method of Oishi by using a decrypted seed to create a block key so that the data does not need to be re-encrypted if the content key is modified.

23. As to claims 2 and 15, $Asano_1$ discloses a system and method for information recording and reproducing, the system and method having:

generates a master key on the basis of the master-key generation information [claim 2] (0011, lines 1-5);

generates two recording keys K1 and K2 (i.e. device unique key) **on the basis of the generated master key** (i.e. LSI key) **and information read out from the information-recording medium** [claim 2] (0026, lines 3-7);

generates a first block key Kb1 (i.e. device unique key) **by carrying out an encryption process based on the generated first recording key K1 and the first seed** [claim 2] (0026, lines 8-10);

decodes encrypted data stored on the information-recording medium by carrying out a decryption process based on the generated second block key Kb2 [claim 2] (0038, lines 2-4; 0052, lines 9-10).

generating a master key on the basis of master-key generation information read out from storage means [claim 15] (0011, lines 1-5);

generating two recording keys K1 and K2 (i.e. device unique key) **on the basis of the generated master key** (i.e. LSI key) **and information read out from the information-recording medium** [claim 15] (0026, lines 3-7);

generating a first block key Kb1 (i.e. device unique key) **by carrying out an encryption process based on the generated first recording key K1 and the first seed** [claim 15] (0026, lines 8-10);

decrypting the encrypted data stored on the information-recording medium by carrying out a decryption process based on the generated second block key Kb2 [claim 15] (0038, lines 2-4; 0052, lines 9-10).

$Asano_1$ does not expressly disclose:

> **acquires a second seed by carrying out a process to decrypt an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1** [claim 2];
>
> **acquiring a second seed by carrying out a process to decrypt an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1** [claim 15].

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by $Asano_1$, as evidenced by Oishi. Oishi discloses a system and method for encrypted data transfer, the system and method having:

> **acquires a second seed** (i.e. content key) **by carrying out a process to decrypt an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1** [claims 2, 15] (0009, lines 8-11) in order to allow for the content key to be changed without requiring re-encryption of the data.

Given the teaching of Oishi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the system and method of $Asano_1$ with the system and method of Oishi by using a decrypted seed so that the data does not need to be re-encrypted if the content key is modified.

$Asano_1$ does not expressly disclose:

generates a second block key Kb2 by carrying out an encryption process based on the acquired second seed and the generated second recording key K2 [claim 2];

generating a second block key Kb2 by carrying out an encryption process based on the acquired second seed and the generated second recording key K2 [claim 15].

$Asano_1$ further discloses a system that **generates a block key by carrying out an encryption process based on the acquired seed and the generated recording key** (i.e. device unique key) [claims 2, 15] (0026, lines 8-10), but does not expressly discloses that a second block key is generated based on a second seed and recording key.

Given the teaching of $Asano_1$, it would have been obvious to a person having ordinary skill in the art at the time the invention was made that generating a second block key using a second set of information is a mere duplication of parts. See MPEP 2144.04.

24. As to claims 3-4, 16-17, $Asano_1$ further discloses a system and method for information recording and reproducing, the system and method having:

generates a first title unique key and a second title unique key on the basis of the master key, a disc ID, which is information read out from the information-recording medium, and two title keys recorded on the information-recording medium [claim 3] (0020, lines 2-7);

generates a first title unique key and a second title unique key on the basis of the master key, a disc ID, which is information read out from the

information-recording medium, and one key seed recorded on the information-recording medium [claim 4] (0020, lines 2-7);

generates a first recording key K1 (i.e. result) **by carrying out an encryption process based on the first title unique key and first information** (i.e. block seed) **read out from the information-recording medium** [claims 3, 4] (0024, lines 7-10);

generating a first title unique key and a second title unique key on the basis of the master key, a disc ID, which is information read out from the information-recording medium, and two title keys recorded on the information-recording medium [claim 16] (0020, lines 2-7);

generating a first title unique key and a second title unique key on the basis of the master key, a disc ID, which is information read out from the information-recording medium, and one key seed recorded on the information-recording medium [claim 17] (0020, lines 2-7);

generating a first recording key K1 (i.e. result) **by carrying out an encryption process based on the first title unique key and first information** (i.e. block seed) **read out from the information-recording medium** [claims 16, 17] (0024, lines 7-10).

Asano$_1$ does not expressly disclose:

generates a second recording key K2 by carrying out an encryption process based on the second title unique key and second information read out from the information-recording medium [claims 3, 4];

generating a second recording key K2 by carrying out an encryption process based on the second title unique key and second information read out from the information-recording medium [claims 16, 17].

Asano$_1$ further discloses a system that **generates a recording key by carrying out an encryption process based on the title unique key and information read out from the information-recording medium** [claims 2-3, 16-17] (0024, lines 7-10), but does not disclose that a second key is created based on a second set of information. Given the teaching of Asano$_1$, it would have been obvious to a person having ordinary skill in the art at the time the invention was made that generating a second recording key using a second set of information is a mere duplication of parts. See MPEP 2144.04.

25. As to claim 9, Asano$_1$ further discloses a system and method for information recording and reproducing, the system and method having:

a first seed serving as key generation information set for each of encryption-processing units composing the encrypted data (0031, lines 1-5);

an encrypted content encrypted on the basis of a second block key Kb1 generated on the basis of the second seed (0017, lines 8-9; 0026, lines 8-10).

Asano$_1$ does not expressly disclose:

a second seed serving as key generation information encrypted on the basis of a first block key Kb2 generated on the basis of the first seed.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the system and method disclosed by $Asano_1$, as evidenced by Oishi. Oishi discloses a system and method for encrypted data transfer, the system and method having:

> **a second seed** (i.e. content key) **serving as key generation information encrypted on the basis of a first block key Kb2 generated on the basis of the first seed** (0009, lines 8-11) in order to allow for the content key to be changed without requiring re-encryption of the data.

Given the teaching of Oishi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the system and method of $Asano_1$ with the system and method of Oishi by using a decrypted seed based on another seed so that the data does not need to be re-encrypted if the content key is modified.

26. As to claims 10-13, $Asano_1$ further discloses a system and method for information recording and reproducing, the system and method having:

> **where the first seed is stored inside control information set for each of encryption-processing units whereas the second seed is stored as encrypted information in a user-data area outside the control information** [claim 10] (0022, lines 2-3; 0023, lines 3-6);
>
> **where the first seed** (i.e. seed) **is stored in a user-data area as unencrypted data whereas the second seed** (i.e. data in block) **is stored in the user-data area as encrypted data** [claim 11] (0023, lines 3-6);

where the encrypted data is a transport stream packet (0018, lines 8-9), **the first seed is stored inside control information for a plurality of transport stream packets** (0018, lines 4-7; 0022, lines 2-3)**, and the second seed is stored as encrypted information inside one of the transport stream packets in a user-data area outside the control information** [claim 12] (0023, lines 3-6);

where the first seed is stored inside a transport stream packet in a user-data area as unencrypted data whereas the second seed is stored as encrypted information inside the transport stream packet in the user-data area [claim 13] (0018, lines 4-10; 0023, lines 3-6).

27. Claims 5-6, 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over $Asano_1$ in view of Asano et al. (US 2002/0085722 A1 and $Asano_2$ hereinafter) and further in view of Oishi.

28. As to claims 5 and 18, $Asano_1$ discloses a system and method for information recording and reproducing, the system and method having:

generating a first block key Kb1 on the basis of a first seed serving as key generation information set for each of encryption-processing units composing the encrypted data stored on the information-recording medium [claims 5, 18] (0031, lines 2-5).

$Asani_1$ does not expressly disclose:

an authentication-processing unit for carrying out an authentication process with the external apparatus to receive the encrypted data read out from the information-recording medium in order to generate a session key Ks [claim 5];

acquiring a second seed by carrying out a process to decrypt an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1 [claims 5, 18];

generating output-use encrypted information by carrying out a process to encrypt data including the second seed on the basis of the session key Ks [claims 5, 18];

where the output-use encrypted information obtained as a result of the process to encrypt data including the second seed on the basis of the session key Ks is output through an interface [claim 5];

carrying out an authentication-processing unit with the external apparatus to receive the encrypted data read out from the information-recording medium in order to generate a session key Ks [claim 18];

outputting the output-use encrypted information obtained as a result of the process to encrypt data including the second seed on the basis of the session key Ks through an interface [claim 18].

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by $Asano_1$, as evidenced by $Asano_2$.

$Asano_2$ discloses a system and method for protecting information by using secret information, the system and method having:

an authentication-processing unit for carrying out an authentication process with the external apparatus to receive the encrypted data read out from the information-recording medium in order to generate a session key Ks [claim 5] (0449, lines 10-11; 0450, lines 1-3) in order to authenticate processes between two systems;

generating output-use encrypted information (i.e. secret communication) **by carrying out a process to encrypt data including the second seed on the basis of the session key Ks** [claims 5, 18] (0451, lines 7-9) in order to provide for authenticated communication between systems;

where the output-use encrypted information obtained as a result of the process to encrypt data including the second seed on the basis of the session key Ks is output through an interface (i.e. between A and B) [claim 5] (0451, lines 7-9) in order to provide for authenticated communication between systems;

carrying out an authentication-processing unit with the external apparatus to receive the encrypted data read out from the information-recording medium in order to generate a session key Ks [claim 18] (0449, lines 10-11; 0450, lines 1-3) in order to authenticate processes between two systems;

outputting the output-use encrypted information obtained as a result of the process to encrypt data including the second seed on the basis of the session key Ks through an interface (i.e. between A and B) [claim 18] (0451, lines 7-9) in order to provide for authenticated communication between systems.

$Asano_1$ in view of $Asano_2$ does not expressly disclose:

acquiring a second seed by carrying out a process to decrypt an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1 [claims 5, 18];

Nonetheless, this feature is well known in the art and would have been an obvious modification of the system and method disclosed by $Asano_1$ in view of $Asano_2$, as evidenced by Oishi.

Oishi discloses a system and method for encrypted data transfer, the system and method having:

acquiring a second seed (i.e. content key) **by carrying out a process to decrypt an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1** [claims 5, 18] (0009, lines 8-11) in order to allow for the content key to be changed without requiring re-encryption of the data.

Given the teaching of $Asano_2$ in view of Oishi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the system and method of $Asano_1$ with the system and method of $Asano_2$

in view of Oishi by encrypting information based on a session key between authenticated systems in order to provide authentication communications and by using a decrypted seed so that the data does not need to be re-encrypted if the content key is modified.

29. As to claims 6 and 19, $Asano_1$ discloses a system and method for information recording and reproducing, the system and method having:

generates a master key on the basis of master-key generation information held by the information-recording medium drive [claim 6] (0011, lines 1-5);

generates two recording keys K1 and K2 (i.e. device unique key) **on the basis of the master key** (i.e. LSI key) **and information read out from the information-recording medium** [claim 6] (0026, lines 3-7);

generates a first block key Kb1 (i.e. device unique key) **by carrying out an encryption process based on the generated first recording key K1 and the first seed** [claim 6] (0026, lines 8-10);

generating a master key on the basis of master-key generation held by an information-recording medium drive [claim 19] (0011, lines 1-5);

generating two recording keys K1 and K2 (i.e. device unique key) **on the basis of the master key** (i.e. LSI key) **and information read out from the information-recording medium** [claim 19] (0026, lines 3-7);

generating a first block key Kb1 (i.e. device unique key) **by carrying out an encryption process based on the generated first recording key K1 and the first seed** [claim 19] (0026, lines 8-10).

$Asano_1$ does not expressly disclose:

acquires a second seed by carrying out a process to decrypt an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1 [claim 6];

generates output-use encrypted information by encrypting data including the second seed and the second recording key K2 on the basis of the session key Ks [claim 6];

outputs the output-use encrypted information including the second seed and the second recording key K2 through an interface [claim 6];

acquiring a second seed by carrying out a process to decrypt an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1 [claim 19];

generating output-use encrypted information by encrypting data including the second seed and the second recording key K2 on the basis of the session key Ks [claim 19];

outputting the output-use encrypted information including the second seed and the second recording key K2 through an interface [claim 19].

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by $Asano_1$, as evidenced by $Asano_2$. $Asano_2$ discloses a system and method for protecting information by using secret information, the system and method having:

generates output-use encrypted information by encrypting data including the second seed and the second recording key K2 on the basis of the session key Ks [claim 6] (0451, lines 7-9) in order to provide for authenticated communication between systems;

outputs the output-use encrypted information including the second seed and the second recording key K2 through an interface [claim 6] (0451, lines 7-9) in order to provide for authenticated communication between systems;

generating output-use encrypted information by encrypting data including the second seed and the second recording key K2 on the basis of the session key Ks [claim 19] (0451, lines 7-9) in order to provide for authenticated communication between systems;

outputting the output-use encrypted information including the second seed and the second recording key K2 through an interface [claim 19] (0451, lines 7-9) in order to provide for authenticated communication between systems.

$Asano_1$ in view of $Asano_2$ does not expressly disclose:

acquires a second seed by carrying out a process to decrypt an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1 [claim 6];

acquiring a second seed by carrying out a process to decrypt an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1 [claim 19].

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by $Asano_1$, as evidenced by Oishi. Oishi discloses a system and method for encrypted data transfer, the system and method having:

acquires a second seed (i.e. content key) **by carrying out a process to decrypt an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1** [claim 6] (0009, lines 8-11) in order to allow for the content key to be changed without requiring re-encryption of the data;

acquiring a second seed (i.e. content key) **by carrying out a process to decrypt an encrypted second seed stored on the information-recording medium on the basis of the generated first block key Kb1** [claim 19] (0009, lines 8-11) in order to allow for the content key to be changed without requiring re-encryption of the data.

Given the teaching of $Asano_2$ in view of Oishi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages

of modifying the system and method of $Asano_1$ with the system and method of $Asano_2$ in view of Oishi by encrypting information based on a session key between authenticated systems in order to provide authentication communications and by using a decrypted seed so that the data does not need to be re-encrypted if the content key is modified.

30. Claims 7-8, 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over $Asano_2$ in view of $Asano_1$.

31. As to claims 7 and 20, $Asano_2$ discloses a system and method for protecting information by using secret information, the system and method having:

> **an authentication-processing unit for carrying out an authentication process with the external apparatus outputting the encrypted data in order to generate a session key Ks** [claim 7] (0449, lines 10-11; 0450, lines 1-3);
>
> **acquiring a seed** (i.e. content key) **used as key generation information and a recording key** (i.e. table key) **by carrying out a process based on the session key to decrypt encrypted information received through the data input interface** [claims 7, 20] (0557, lines 9-15);
>
> **carrying out an authentication process with the external method outputting the encrypted data in order to generate a session key Ks** [claim 20] (0449, lines 10-11; 0450, lines 1-3);

$Asano_2$ does not expressly disclose:

generating a block key to be used as decryption key for decryption of encrypted data by carrying out an encryption process based on the seed and the recording key [claims 7, 20];

carrying out a process based on the block key to decrypt encrypted data [claims 7, 20].

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by $Asano_2$, as evidenced by $Asano_1$. $Asano_1$ discloses a system and method for information recording and reproducing, the system and method having:

generating a block key to be used as decryption key for decryption of encrypted data by carrying out an encryption process based on the seed and the recording key (i.e. device unique key) [claims 7, 20] (0026, lines 8-10) in order to recreate a key with which to restore original data;

carrying out a process based on the block key to decrypt encrypted data [claims 7, 20] (0052, lines 9-10) in order to restore original data.

Given the teaching of $Asano_1$, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the system and method of $Asano_2$, with the system and method of $Asano_1$ by creating a block key from supplied data so that original data can be restored.

32. As to claims 8 and 21, $Asano_2$ discloses a system and method for protecting information by using secret information, the system and method having:

an authentication-processing unit for carrying out an authentication process with the external apparatus to receive the encrypted data read out from the information-recording medium in order to generate a session key Ks [claim 8] (0449, lines 10-11; 0450, lines 1-3);

generating output-use encrypted information by carrying out a process to encrypt the decrypted data on the basis of the generated session key Ks [claims 8, 21] (0557, lines 5-7);

where the output-use encrypted information obtained as a result of the process to encrypt the decrypted data on the basis of the session key Ks is output through an interface [claim 8] (0557, lines 5-11);

carrying out an authentication process with the external method to receive the encrypted data read out from the information-recording medium in order to generate a session key Ks [claim 21] (0449, lines 10-11; 0450, lines 1-3);

outputting the output-use encrypted information obtained as a result of the process to encrypt the decrypted data on the basis of the session key Ks through an interface [claim 21] (0557, lines 5-11).

Asano$_2$ does not expressly disclose:

generating a block key on the basis of a seed serving as key generation information set for each of encryption-processing units composing the encrypted data stored on the information-recording medium [claims 8, 21];

acquiring decrypted data by carrying out a process to decrypt the encrypted data stored on the information-recording medium on the basis of the generated block key [claims 8, 21].

Nonetheless, these features are well known in the art and would have been an obvious modification of the system and method disclosed by $Asano_2$, as evidenced by $Asano_1$. $Asano_1$ discloses a system and method for information recording and reproducing, the system and method having:

generating a block key on the basis of a seed serving as key generation information set for each of encryption-processing units composing the encrypted data stored on the information-recording medium [claims 8, 21] (0031, lines 2-5) in order to recreate a key with which to restore original data;

acquiring decrypted data by carrying out a process to decrypt the encrypted data stored on the information-recording medium on the basis of the generated block key [claims 8, 21] (0052, lines 9-10) in order to restore original data with a key that was not directly transmitted with the data.

Given the teaching of $Asano_1$, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the system and method of $Asano_2$, with the system and method of $Asano_1$ by creating a block key from supplied data so that original data can be restored with a key that was not directly transmitted with the data.

Prior Art Made of Record

33. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Asano et al. (US 2002/0169971 A1) discloses a system for data authentication.

b. Asano et al. (US 2003/0095664 A1(discloses a system and method for information recording and playback.

c. Ohmori et al. (US Patent No. 6,459,792 B2) discloses a system for cryptographic processing using a block cipher.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Walter Benson can be reached on (571) 272-2227. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

26 March 2008

/Sarah Su/
Examiner, Art Unit 4158

/Uyen-Chau N. Le/
Primary Examiner, Art Unit 4158